FortiClient (Windows) - Release Notes

Version 6.0.5

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

January 31, 2019
FortiClient (Windows) 6.0.5 Release Notes
04-605-533962-20190131

TABLE OF CONTENTS

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.0.5 build 0209.

Review all sections prior to installing FortiClient.

Licensing

FortiClient offers two licensing modes:

- Standalone mode
- Managed mode

Standalone mode

In standalone mode, FortiClient is not connected to a FortiGate or FortiClient Enterprise Management Server (EMS). In this mode, FortiClient is free for private individuals and commercial businesses to use. No license is required.

Support for FortiClient in standalone mode is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided.

Managed mode

Companies with large installations of FortiClient usually need a means to manage their endpoints. EMS can be used to provision and centrally manage FortiClient endpoints, and FortiGate can be used with FortiClient endpoints for network security. Each FortiClient endpoint can connect to a FortiGate or an EMS. In this mode, FortiClient licensing is applied to the FortiGate or EMS. No separate license is required on FortiClient itself.

When using the ten free trial licenses for FortiClient in managed mode, support is provided on the Fortinet Forums. Phone support is not provided when using the free trial licenses. Phone support is provided for paid licenses.

FortiClient licenses on the FortiGate

FortiGate 30 series and higher models include a FortiClient free trial license for ten connected FortiClient endpoints. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

FortiClient licenses on the EMS

EMS includes a FortiClient free trial license for ten connected FortiClient endpoints for evaluation. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

Special Notices

Nested VPN tunnels

Parallel, independent VPN connections to different sites are not supported; however, FortiClient VPN connection may still be established over existing third-party (for example, AT&T Client) VPN connection (nested tunnels).

Microsoft Windows Server support

For Microsoft Windows Servers, the AV and Vulnerability Scan features for FortiClient are supported.

FortiClient Rebranding Tool not supported

FortiClient (Windows) 6.0.5 does not support the FortiClient Rebranding Tool.

Installation Information

Firmware images and tools

The following files are available in the firmware image file folder:

File	Description
FortiClientSetup_6.0.xx.xxxx.exe	Standard installer for Microsoft Windows (32-bit)
FortiClientSetup_6.0.xx.xxxx.zip	A zip package containing FortiClient.msi and language transforms for Microsoft Windows (32-bit). Some properties of the MSI package can be customized with FortiClient Configurator Tool.
FortiClientSetup_6.0.xx.xxxx_x64.exe	Standard installer for Microsoft Windows (64-bit)
FortiClientSetup_6.0.xx.xxxx_x64.zip	A zip package containing FortiClient.msi and language transforms for Microsoft Windows (64-bit). Some properties of the MSI package can be customized with FortiClient Configurator Tool.
FortiClientTools_6.0.xx.xxxx.zip	A zip package containing miscellaneous tools, including VPN automation files

The following tools and files are available in the FortiClientTools_6.0.xx.xxxx.zip file:

File	Description
FortiClientVirusCleaner	A virus cleaner
OnlineInstaller	This file downloads and installs the latest FortiClient file from the public FDS
SSLVPNcmdline	Command line SSL VPN client
SupportUtils	Includes diagnostic, uninstallation, and reinstallation tools
VPNAutomation	A VPN automation tool

Review the following sections prior to installing FortiClient version 6.0.5: Introduction on page 4, Special Notices on page 6, and Product Integration and Support on page 9.

Installation options

When installing FortiClient version 6.0.5, you can choose the setup type that best suits your needs. FortiClient will always install the Fortinet Security Fabric Agent (SFA) feature and enable the Vulnerability Scan feature by default. You

can select to install one or more of the following options:

- Secure Remote Access: VPN components (IPsec and SSL) will be installed.
- Advanced Persistent Threat (APT) Components: FortiSandbox detection and quarantine features will be installed.
- Additional Security Features: Select one or more of the following to install them: AntiVirus, Web Filtering, Single Sign On, Application Firewall

It is recommended to not install VPN components on Windows Server systems if not required.

Upgrading from previous FortiClient versions

FortiClient version 6.0.5 supports upgrade from FortiClient versions 5.4 and later.

If you are deploying an upgrade from FortiClient 5.6.2 or earlier versions via FortiClient EMS and the upgrade fails, uninstall FortiClient on the endpoints, then deploy the latest version of FortiClient.

Downgrading to previous versions

Downgrading FortiClient version 6.0.5 to previous FortiClient versions is not supported.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal. After logging in, click on *Download* > *Firmware Image Checksums*, enter the image file name, including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiClient 6.0.5 support information

The following table lists version 6.0.5 product integration and support information.

Desktop Operating Systems	• Microsoft Windows 7 (32-bit and 64-bit) • Microsoft Windows 8, 8.1 (32-bit and 64-bit) • Microsoft Windows 10 (32-bit and 64-bit) FortiClient 6.0.5 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server Operating Systems	• Microsoft Windows Server 2008 R2 or newer FortiClient 6.0.5 does not support Windows Server Core.
Minimum System Requirements	• Microsoft Windows compatible computer with Intel processor or equivalent • Compatible operating system and minimum 512MB RAM • 600MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dial-up connections • Ethernet network interface controller (NIC) for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for viewing FortiClient documentation • Windows Installer MSI installer version 3.0 or later
FortiAnalyzer	• 6.0.0 and later • 5.6.0 and later
FortiAuthenticator	• 4.3.1 • 4.3.0 • 4.2.1 FortiToken Mobile push notification is not supported for the following versions: • 4.2.0 • 4.1.0 and later • 3.3.0 and later • 3.2.0 and later • 3.1.0 and later • 3.0.0 and later
FortiClient EMS	• 6.0.0 and later
FortiManager	• 6.0.0 and later • 5.6.0 and later
FortiOS	• 6.0.0 and later • 5.6.0 and later Only IPsec VPN and SSL VPN are supported with the following FortiOS versions:

	• 5.4.0 and later
FortiSandbox	• 3.0.0 and later • 2.5.0 and later The following version is supported, but may require authorization of FortiClient to be disabled. To disable authorization run the FortiSandbox CLI command: `device-authorization -f` • 2.4.0 and later The following supported versions do not offer authorization of FortiClient: • 2.3.0 and later • 2.2.0 and later • 2.1.0

Language support

The following table lists FortiClient language support information.

Language	Graphical user interface	XML configuration	Documentation
English	Yes	Yes	Yes
Chinese (simplified)	Yes		
Chinese (traditional)	Yes		
French (France)	Yes		
German	Yes		
Japanese	Yes		
Korean	Yes		
Portuguese (Brazil)	Yes		
Russian	Yes		
Spanish (Spain)	Yes		

The FortiClient language setting defaults to the regional language setting configured on the client workstation, unless configured in the XML configuration file.

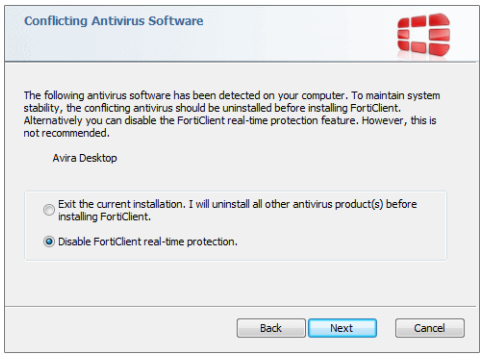
If the client workstation is configured to a regional language setting that is not supported by FortiClient, it defaults to English.

Conflicts with third party antivirus products

The antivirus feature in FortiClient is known to conflict with other similar products in the market.

- FortiClient's antivirus feature should not be used with other AV products.
- If not using FortiClient's antivirus feature, the FortiClient installation folder should be excluded from scanning for the third party AV product.

During a new installation of FortiClient, the installer will search for other registered third party software and, if any is found, warn users to uninstall them before proceeding with the installation. There is also an option to disable FortiClient Real Time Protection (RTP).



Resolved Issues

The following issues have been fixed in version 6.0.5. For inquiries about a particular bug, contact Customer Service & Support.

Endpoint Control

Bug ID	Description
515473	Hiding any feature (except Application Firewall) causes FortiClient (Windows) to report the feature as *Installed* and not *Enabled*.
519481	FortiClient does not parse the FortiGate serial number when configured in high availability and reports wrong on/off-net status when using the DHCP on-net feature.
533673	FortiClient endpoints Anti Virus/Web Filter/Sandbox/Firewall events not shown in *Endpoints* screen.
534786	Pre-prepared package - No Security Fabric Agent - Logging Telemetry should not be enabled.

Malware Protection

Bug ID	Description
526229	FortiClient Anti Virus is locking Microsoft Office files and not allowing them to save.

Remote Access

Bug ID	Description
481361	VPN before Logon does not appear on Windows 10 x64 after enabling even after reboot.
514115	FortiClient (Windows) lost saved password after upgrading from 5.6.x and disconnecting an auto-connected IPsec VPN.
516244	Changing/saving VPN settings removed IPv6 `<remote_networks><network>`.
521198	Username and password get deleted on IPsec VPN when a profile change is done on EMS.
526286	Complex preshared secret will not work if entered via GUI.

Bug ID	Description
531647	VPN auto-connect logic not restored after manual connection.
532838	SSL VPN failed to save setting for save logon for SSL VPN.
532942	VPN before logon not working (FortiClient syncs with EMS profile but even after that at logon page unable to see FortiClient VPN icon).

Vulnerability Scan

Bug ID	Description
526401	User still allow to start vcm scan when update_task was running.
531020	Fortisetting daemon expose pipe allows low privilege programs to change FortiClient (Windows) settings.
531077	Remove os.exec, open from Vulnerability Scan signature.

GUI

Bug ID	Description
495880	Non-admin domain users can stop/pause USB media scans enforced by EMS configuration.
527471	FortiClient (Windows) GUI displays content of any text file .
531361	*Unlock Settings* button on GUI will not ask for admin.

Install and upgrade

Bug ID	Description
528590	Alert when updates available is *ON* despite `<config auto_patch>` and `<update_action>` being disabled.
534103	FortiClient lost USB monitor setting after upgrade from 6.0.4 to 6.0.5
535192	FortiClient (Windows) failed to update firmware when using custom FDS server

Other

Bug ID	Description
518771	FortiShield blocks Forticlient.exe from changing registry - FA_Scheduler.
525811	FortiClient blocks access to files on mapped home drives.
534306	Able to replace the .exe files in the FortiClient installation folder.
535392	FortiClientSSO.msi was not digitally signed.

Known Issues

The following issues have been identified in FortiClient (Windows) 6.0.5. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Endpoint Control

Bug ID	Description
519995	FortiClient (Windows) profile has certificates when EMS profile does not
525062	FortiClient stopped receiving IP list from EMS.

Malware Protection

Bug ID	Description
489370	Email alerts are incomplete for malicious website events.
513213	AntiExploit Engine blocking legitimate applications.
514009	FortiClient failed to inject into Firefox application.
516704	Anti Virus should recognize Windows-signed files.
525034	FortiClient does not scan on next start-up if off during scheduled scan time.
531398	Unable to restore from EMS file quarantined by Sandbox scan.
533840	FortiClient Anti Virus /Anti-Exploit make Internet Explorer not work. It will not start or it will start and crash.

Application Firewall

Bug ID	Description
516092	Unable to block PsExec communication/traffic.
517351	Application gets blocked when Firewall is enabled.
526255	Application Firewall interrupting "Architect" application without any block.

Remote Access

Bug ID	Description
525449	JavaScript error while connecting VPN, issue on version 6.0.X was occurring due to admin roaming profile.
525460	On FortiClient (Windows) 6.0.3 autoconnect does not retry to connect if the connection fails the first time.
525542	After laptop boot or wake-up, FortiClient (Windows) will try to autoconnect even though it is onnet.
528434	Failed to see VPN before logon option on Win10x64 1803 with fresh install of FortiClient.
532542	IPsec state is disconnected, but FortiTray has the lock sign.
533022	Changing VPN tunnel name in EMS GUI can result in partial configuration loss.
534650	`<allow_standard_user_use_system_cert>` does not work for SSL VPN IPv6.
535114	Unable to select user certificate when reconnecting to a managed SSL VPN profile.
535767	*Save Password/Credentials* checkbox for SSL VPN only checked if always up is enabled.

Vulnerability Scan

Bug ID	Description
510597	FortiClient (Windows) failed to patch OS vulnerabilities on Windows 10 x64 platform with existing outstanding Windows update.

GUI

Bug ID	Description
526216	FortiClient GUI reports incorrect threats in Real Time Protection.
535903	VPN name, IP address, and username are hidden when "\" is used in the VPN tunnel username.

Install and upgrade

Bug ID	Description
531392	FortiClient upgrade removes Sandbox quarantined files and submitted files statistics.

Bug ID	Description
536215	FCInstallerLight.exe crashed when FortiClient (Windows) tried to upgrade from FortiTray with standard user.

Other

Bug ID	Description
513932	No CERT payload sent by FortiClient during IKE2 certificate authentication.
520808	FortiClient failing certificate validation due to ignored intermediate CA.
524127	Event messages and context are duplicated and incorrect.
524463	FortiShield blocks Forticlient.exe to change file - undefined.log.
525021	FortiClient fails to find avatar when logged in as domain user.
532068	FortiClient cannot see the certificate when the subject of certificate contain diacritics.
534439	Faulting application name: fortifws.exe Crash caused by libips.dll.
534815	Unable to run FCRemove in unattended mode.

Change Log

Date	Change Description
2019-01-31	Initial release of FortiClient (Windows) 6.0.5.